

TECHNICAL RESEARCH REPORT

Routing Algorithms in All-Mobile Wireless Networks

by A. Michail, A. Ephremides

CSHCN T.R. 97-2
(ISR T.R. 97-13)



The Center for Satellite and Hybrid Communication Networks is a NASA-sponsored Commercial Space Center also supported by the Department of Defense (DOD), industry, the State of Maryland, the University of Maryland and the Institute for Systems Research. This document is a technical report in the CSHCN series originating at the University of Maryland.

Web site <http://www.isr.umd.edu/CSHCN/>

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 1997		2. REPORT TYPE		3. DATES COVERED -	
4. TITLE AND SUBTITLE Routing Algorithms in All-Mobile Wireless Networks				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Army Research Laboratory, 2800 Powder Mill Road, Adelphi, MD, 20783				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT see report					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 6	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

ROUTING ALGORITHMS IN ALL-MOBILE WIRELESS NETWORKS *

Anastassios Michail
Anthony Ephremides

Electrical Engineering Department and Institute for Systems Research
University of Maryland
College Park, Maryland

ABSTRACT

In networks with mobile radio nodes in which connectivity varies rapidly with time, it is necessary to develop algorithms for identifying and maintaining paths between communicating pairs of nodes. Motivated by earlier work that accomplishes such a task for datagram packet service, we develop a similar algorithm for connection-oriented service. The algorithm establishes circuit routes for initial connection based on a mechanism of short packets exchange and takes advantage of the possibility to convert a connectivity change into a “soft” failure to maintain and re-route on-going sessions. In this paper we give a presentation of the algorithm which is currently undergoing extensive simulation-based evaluation.

I. INTRODUCTION

We consider the routing problem in a large, all-mobile wireless network that models units deployed in the Digital Battlefield. We are interested in establishing and maintaining paths between mobile nodes for the transmission of messages (for both connection-less datagram service and connection-oriented service). Without restricting our case to networks with a priori known architecture (e.g. cellular radio systems), we examine general purpose military communication networks. Such networks are subject to frequent and unpredictable connectivity changes and links between mobile nodes are bandwidth-constrained. In such environments it is important to establish algorithms that are capable of sustaining the desired end-to-end service. We propose a distributed algorithm that is designed to perform for any set of nodes with the same functionalities without the need of global connectivity information.

*Prepared through collaborative participation in the Advanced Telecommunications/Information Distribution Research Program (ATIRP) Consortium sponsored by the U.S. Army Research Laboratory under Cooperative Agreement DAAL01-96-2-0002.

The starting point of our approach is a distributed routing algorithm for data packet service that was presented in [1] and to which we will refer as CE algorithm. This algorithm assumes adequate bandwidth and an underlying access protocol that is interference-free. It relies on the execution by all nodes and separately for each potential destination of a two-phase procedure. The first phase involves the flooding of a “query” message that is initiated by a source node in search of a path to a designated destination node. This message generates the reverse flooding of a “reply” message as soon as the destination node location is determined. The result is the establishment of a directed graph on a subset of the network that is “rooted” at the destination node and thus provides an initial set of routes. The second phase involves a similar structured exchange of messages to react to the “failure” of an element of the previously established route and is intended to discover a new “by-pass” route. The algorithm is deadlock-free and is capable of detecting catastrophic separation of the network.

In this paper, we shift our focus to session-oriented service and, as is natural in this case, to the core of limited available bandwidth. We present a new algorithm that establishes circuit routes for initial connection in the manner of the preceding data algorithm but that reacts differently, as it should, in the case of a failure, or connectivity change. The algorithm must avoid loops and deadlocks as in [1] and, in this case, it is modified to include in the message exchange information on the availability of resources. In addition, in order to maintain on-going sessions in the presence of topological changes the algorithm takes advantage of the possibility to convert a wireless connectivity change to a “soft” failure by means of adaptive information rate control. Because the emphasis is on the logic and the distributed, deadlock-free nature of the algorithm, many details that pertain to the physical layer communications are simplified or deferred for future con-

sideration. A preliminary description of our work was presented in [2].

The rest of the paper is structured as follows. Section II introduces some necessary terminology and notation along with basic assumptions about the network model. Section III gives a high-level description of the algorithm followed by a detailed presentation of its operation, section IV briefly presents the simulation setup and finally section V concludes with a short discussion of the algorithm.

II.NETWORK MODEL

The network is modeled as a graph $G = (N, L)$, where N is a finite set of nodes and L is the set of links. Each node $i \in N$ has a unique node identifier (ID) and two-way communication is allowed over each link $(i, j) \in L$. All nodes are mobile and the status of the communication links is a function of nodes' location, distance, transmission power levels, channel interference and antenna patterns. Due to these factors, the set of links L is changing with time.

An underlying link-level protocol is assumed which assures distributed knowledge of the connectivities' changes – in the sense that each node i is aware of all its adjacent nodes at all times – and that transmitted packets are received correctly and simultaneous two-way transmission over a link that would cause interference does not occur. The mechanism of this link-level protocol operation will be addressed at a future time. All the nodes adjacent to a node i are referred to as its neighbors. For each neighbor j of node i there exists a link between j and i which can either be undirected or directed. In the second case, if the link is directed from i to j it is characterized as downstream (DN) and j is a downstream neighbor of i . Similarly, if the link is directed from j to i it is characterized as upstream (UP) and j is an upstream neighbor of i .

III.ALGORITHM DESCRIPTION

A. Overview of operation

We consider multiple independently executing versions of the distributed routing CE algorithm, each one of them running for a specific destination node. A corresponding version of the new algorithm is overlaid on top of each such version and utilizes information provided by the underlying routing protocol to request connections through existing routes.

Algorithm execution can be viewed in two logical phases, the “Construction phase” and the “Maintenance phase” which occur simultaneously in a dynamic

topology. During the construction phase mobile nodes place requests for connection to specific destination nodes along routes provided by concurrent execution of the underlying CE algorithm, and sessions are established upon availability of network resources. All nodes maintain a database with information on the current optimal (in terms of available resources) paths to all destinations, based on which future decisions among paths can be made. Note that bandwidth constraints of a link are determined by the number of available transceivers at the edges of the link in contrast to fixed-link networks where bandwidth availability depends on link capacity.

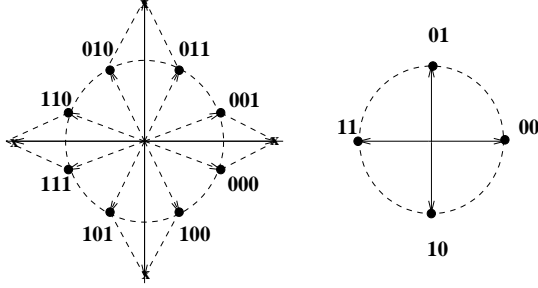
During the maintenance phase the algorithm reacts to connectivity changes that affect on-going sessions. In packet radio networks, upon a link failure new routes are identified and invalid routes are erased. In our case, since a voice or video connection must not be “dropped” or interrupted the algorithm takes advantage of the possibility to convert a wireless connectivity change to a “soft” failure, maintaining the on-going session until a new path is discovered by the affected nodes. Of course, when a “hard” link failure takes place, possibly because of a node failure or because of jamming, connectivity is automatically lost and the source node needs to re-establish the connection. In the following paragraph we propose a mechanism to maintain links affected by topological changes.

B. Adaptive Transmission Rate

A “link-failure” in a wireless environment usually occurs when the energy-per-bit-to-interference ratio falls below a predetermined threshold. In order to maintain connectivity between two nodes in the presence of topological changes, and to avoid the use of a power control mechanism which may aggravate interference and cause additional connectivity fluctuations, we propose a technique of adaptive transmission rate. In fact the information rate can be adjusted at the receiver by means of either hierarchical encoding at the source or adaptive demodulation at the receiver. Thus, the receiver can unobtrusively boost the value of this ratio by “gleaning” out of the received signal a somewhat degraded version at a reduced rate.

Suppose for example that the transmitted information is encoded in Multiple Phase Shift Keying (MPSK) and for purposes of illustration consider $M=8$. A node which senses quality degradation in one of its DN links, does not need to notify the transmitting source to adjust the rate by any exchange of control messages although it has that option. Instead it starts decoding

the received signal as a QPSK by summing in pairs the output of the matched filters in a way shown in figure 1(a).



(a) 8-phase signal constellation (b) equivalent 4-phase constellation

Figure 1: Constellation Diagrams for 8-PSK and QPSK

The probability of error per symbol for QPSK is approximated by [3]

$$P_4 = 2Q \left(\sqrt{\left(\frac{E_s}{N_o} \right)_4} \right) \quad (1)$$

while the probability of error per symbol for 8-PSK is approximated by [3]

$$P_8 = 2Q \left(\sqrt{2 \left(\frac{E_s}{N_o} \right)_8} \sin \frac{\pi}{8} \right) \quad (2)$$

The relationship between $\left(\frac{E_s}{N_o} \right)_8$ and $\left(\frac{E_s}{N_o} \right)_4$ can be calculated by performing the appropriate analysis. If we compare formulas (1) and (2) we get an improved symbol error rate when the decoder switches to QPSK. For example, if the probability of symbol error is $P_8 = 10^{-2}$, switching from 8-PSK to QPSK gives probability of symbol error $P_4 \simeq 2 \cdot 10^{-6}$ which is a significant improvement for a voice session. Hence the first two bits of each symbol can be detected with a smaller probability of error compared to the probability of error for the original symbol.

The method that is proposed in this section trades off signal quality for algorithm efficiency. If we have a voice connection or a video transmission the reduction in transmission rate will result in a degraded version of the transmitted signal but the connection is not lost and the quality will possibly improve either because the session will be served by another path, or because the link will recover. Of course, it is necessary to confirm whether the more reliable reconstruction of the degraded signal is of preferable quality than the less reliable reconstruction of the full-rate signal that would correspond to taking no action at all. In fact, the use of intelligent mapping of bits to symbols and/or the use of hierarchical compression [4], along with the use

of efficient bit allocation algorithms [5], can be coupled with our technique to improve overall performance. The trade-offs involved in maintaining the best signal quality while adjusting adaptively the demodulation as well as choosing signal constellations are the subject of a separate study.

C. Detailed Description

Each node maintains a connectivity table which contains for every destination multiple entries of the form

Connect-ID	IN link	OUT link	Tx.Rx-ID
------------	---------	----------	----------

with the connection ID number, the incoming and outgoing link and the transceiver ID that serves the session. The mobile node is also aware of the current decoding scheme and the number of idle transceivers.

Construction Phase

Without loss of generality we examine one version of the algorithm executing for the destination node denoted DEST, and we assume that at some point in time a node, not adjacent to the DEST, will desire a connection. We also assume that this node has multiple DN links, which implies that there exists at least one route to the DEST.

The node desiring the connection generates a Connection-Request (CR) packet (see example Fig. 2). A CR is a control packet that consists of a source node identifier (ID), a destination node ID, a transmitting node ID and a connection ID which will be useful to distinguish the request from other requests placed by the same node, but also in the connectivity table entries at the nodes. The CR is transmitted over one of the existing DN links. The selection is based on the information about transceivers' availability that has already been collected by previous control messages exchange and the node chooses to transmit among all DN nodes to the one that is in the path with the maximum number of available transceivers. If we are in an initial stage and no such information has already become available, the selection is made randomly.

Upon receiving a CR packet, a node may react in three different ways.

- If it has an idle transceiver and it is not the destination node it retransmits the CR over one of its DN links, after updating the corresponding entry in the connectivity table and temporarily reserving the transceiver (Fig. 2(b)).

- If the node does not have any available transceivers at that moment, it will generate and transmit to the

UP neighbor a Negative Acknowledgment (NAK) and block that particular link until a transceiver becomes available (Fig. 2(d)). The NAK is a control packet that consists of the source node ID, the destination node ID and the connection ID. When a node receives a NAK over a DN link, it has to repeat the construction phase using some other DN link, or re-transmit the NAK UP if all DN links are blocked or unavailable.

– If it is the destination node and can accommodate the connection, it generates and transmits backwards an Acknowledgment (ACK) packet. (Fig. 2(f)). The ACK is a control packet that consists of the source ID, the destination ID, the connection ID and an entry representing the available number of transceivers in the full path to the DEST, the usefulness of which will be explained later.

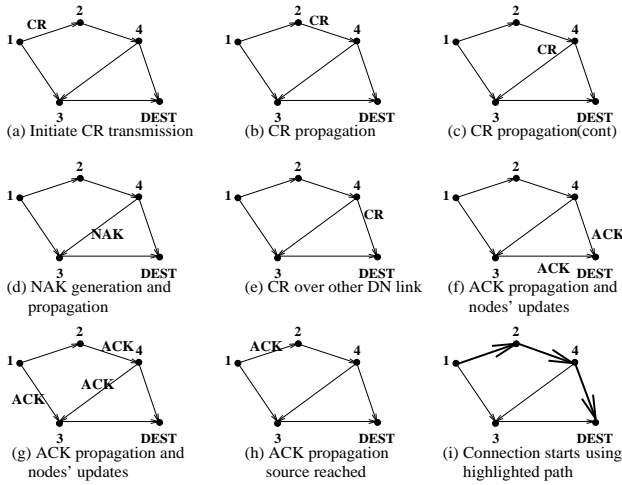


Figure 2: Construction phase, CR, NAK and ACK propagation

The idea hidden behind this control packet exchange is the collection of information - individually by every node - about resources available in paths originating from the node and terminating at the DEST. We consider two different ways of doing this. First by flooding of the ACK in the network and second with short update messages broadcast, by every node that changes number of idle transceivers, to all its neighbors. In the first case the ACK plays the role of an update packet since it carries the maximum number of available transceivers, updates it (after comparing to the number in the current node) and broadcasts it over all UP links until all nodes have received it (Fig. 2(f) - (i)). Nodes that have placed reservation for the specific request execute the additional step of confirming the establishment of the connection. In the second case the ACK follows only the path along which the request was placed and all the nodes in that path have to broadcast short up-

date packets to their neighbors. The latter mechanism avoids unnecessary flooding of control packets but may increase the number of unsuccessful requests, whereas the former mechanism provides the maximum amount of needed information, with the risk that it might be inaccurate if the arrival rate of connection requests is high. That will be the case if other – simultaneously executing – versions of the algorithm result in updates at same nodes.

Maintenance Phase

During the maintenance phase the algorithm utilizes a Connection-Handoff (CH) control packet to discover new or “by-pass” paths and “re-route” a session (see example Fig. 3). A CH consists of the source node ID, the transmitting node ID and the connection ID, and it is transmitted by a node when one of its DN links that is being used by an on-going session demonstrates a poor quality. The CH is transmitted over one of the node’s DN links, other than the one used by the session. In the construction phase description, the node would choose over which DN link to transmit a CR based on transceivers’ availability in the whole path to the DEST. In the maintenance phase this is not necessarily a correct approach. Many CH’s may fail because of lack of transceivers even though some of those transceivers will still be reserved for the same session and could be reused (since the connection is still in progress utilizing network resources). Hence, we have the option of selecting one DN link based on bandwidth information – with a high chance of failure – or of making a random choice. Both options will be simulated and compared.

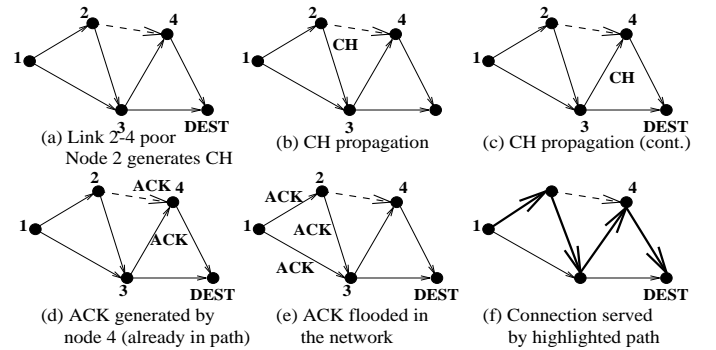


Figure 3: Maintenance phase, CH, ACK and NAK propagation because of soft failure of link 2-4-DEST

Receiving a CH implies in general reaction in a similar way to receiving a CR. Note however that a CH refers to an on-going session and not to a new request (since resources have already been reserved for this ses-

sion) and for that reason a node receiving a CH checks if the connection ID is in its connectivity table. If so, the node will generate and transmit an ACK only if it is located in the segment of the path beyond the poor quality link (Fig. 3(d)). In fact if the node that just received the CH was decoding in 8-PSK, it is located in that segment of the path that has not been affected by the link degradation and the CH request will fail, whereas if it was decoding in QPSK and it is not the node that initially generated the CH, it is located beyond the affected link and can generate an ACK since the rest of the path to the DEST can still be used.

The rest of the nodes that are not participating in the current connection react to a CH in the same manner they would do for a CR. The CH propagation continues until an ACK is generated in reply to the CH. If a node has exhausted all its DN links without receiving any ACK, then it has to transmit the CH over the UP link of the session, and the upstream node will repeat the CH procedure.

IV.SIMULATION

The proposed algorithm is presently undergoing extensive simulation-based evaluation in Opnet/Modeler Radio ¹. For the simulation setup we assume an underlying non-blocking channel access scheme which applies to the control channel allowing as many nodes as possible to transmit, provided no primary or secondary collisions occur.

We simulate the algorithm in a variety of network architectures and environments in which node connectivities are not static but vary with time. Links may totally fail, degrade or recover independently and according to the model assumed for topological changes. The network can also be vulnerable to jamming and some portions may be disconnected or severely affected due to the existence of jammers. We consider the rate of topological change to be a parameter in the simulation. We build simulations by assuming topologies with relatively small number of mobile nodes but we also simulate network operation in larger networks and in chaotic situations with hundreds of thousands of mobile nodes.

Various types of traffic are supported, including datagram traffic, voice connections, file transfers and multimedia traffic. Connection-oriented service is of higher priority since dedicated bandwidth is assigned to the accepted connections. Datagram traffic will be routed

only if there are available transceivers and according to the rules of the underlying data protocol.

The algorithm is evaluated by studying its reaction time to connectivity changes as a function of the rate of topological change, and by collection of statistics for percentage of connection-requests blocked or of sessions interrupted.

V.CONCLUSION

We presented a distributed algorithm that identifies and maintains paths between mobile nodes in a wireless network with varying topology, for both connection-less datagram service and connection-oriented service. Algorithms that perform such a task for packet routing can usually maintain more than one routes from source to destination, having thus more flexibility and robustness to topological changes. In our case we focused on connection-oriented service where the maintenance of connectivity becomes more crucial. We proposed a mechanism of adaptive information rate which can be used to maintain on-going connections while a search for alternative paths is performed. In the future we plan to continue evaluation of the algorithm with extended simulation, and provide a theoretical validation.

"The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government."

REFERENCES

- [1] M. S. Corson, and A. Ephremides, "A Distributed Routing Algorithm for Mobile Wireless Networks," *Wireless Networks*, Vol. 1, pp. 61-81, 1995.
- [2] A. Michail, and A. Ephremides, "Algorithms for Establishing and Maintaining Sessions in Wireless Networks with Changing Connectivity," 34th Annual Allerton Conference on Communications Control and Computing, Oct. 1996.
- [3] J. G. Proakis, and M. Salehi, *Communications Systems Engineering*, Prentice-Hall, 1994.
- [4] M. B. Pursley, "Signaling Methods and Routing Techniques for Mobile, Multimedia, Wireless Networks: An Overview of Recent Research Results," Workshop on New Techniques for Radio Communications and Wireless Networks, San Diego, CA, Sep. 1996.
- [5] E. Perahia, C. Wang, C. J. Hansen, and G. J. Pottie, "Interference Suppression Using Antenna Arrays and Dynamic Power and Bit Allocation," *Proceedings of Interference Rejection and Signal Separation in Wireless Communications (IRSSWC) Symposium*, New Jersey Institute of Technology, Mar. 1996.

¹Opnet Modeler/Radio is a trademark of MIL3 Inc.